Annual 47 C.F.R. 64.2009(e) CPNI Certification

EB Docket 06-36

Commission's Secretary, Marlene H. Dortch
Office of the Secretary, Federal Communications Commission
445 12th Street SW
Suite TW-A325
Washington DC 20554

Annual 47 C.F.R. 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: Wednesday, February 25, 2009

Name of company covered by this certification: BigCity Networks, Inc.

Form 499 Filer ID: 826065

Name of signatory: Jeff Swickard

Title of signatory: CEO

I, Jeff Swickard, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed _____

Jeff Swickard
CEO

Description of CPNI Policies and Procedures

I. **Overview.**

BigCity Networks, Inc. ("BCN") is a regional voice over IP ("VoIP") telephony company, primarily serving the Houston, Dallas, Austin, and San Antonio, Texas markets with a focus on small to medium sized businesses. BCN's VoIP services include local and long distance dial tone. With regard to this relatively small customer base, BCN has knowledge of end user CPNI only insofar as it has information that it uses to bill its customers. Nevertheless, protecting even this limited end user CPNI is important to BCN and the company has adopted various operational procedures to assure that, consistent with the Commission's rules, the CPNI that it holds is protected from unauthorized or illegal use, access and disclosure. Jared Martin, the Corporate Secretary and Executive Vice President, is currently responsible for maintaining the security of CPNI.

II. **Electronic Security.**

The company has security measures in place to protect data from external attacks to its website and improper verbal requests for data via personal contacts with BCN's Customer Care and Billing Departments. BCN currently does not have a customer web portal for telephony services and therefore does not allow customers to view traffic data on-line. If/when BCN implements an updated website and a customer web portal for telephony services, it is anticipated that the web portal will have login/password security and will use encryption to ensure the security of this information. Any such web portal would limit customers to accessing their specific data only.

III. **Access to CPNI.**

The company has procedures in place that allow only customers of record to obtain customer confidential information (i.e. specific call detail records). BCN has policies in place to limit access to CPNI by customers. Customer requests for CPNI are not accepted via the telephone. Any request for sensitive information must be submitted in writing and come from the contact of record for the customer. When information is released to the customer, it is sent via postal mail to the customer's address of record.

Upon establishing an account with BCN, customers are required to provide a password that does not contain any personally identifiable information (i.e. last four digits of SSN or a maiden name). Instead, customers must provide a unique password that cannot be easily associated with the customer. When submitting requests to release sensitive information, the customer must

provide the account password in their request. Further, any calls to BCN's Billing Department requires that the customer authenticate themselves before discussing their account. A separate customer password is established for Help Desk calls. BCN requires customers to authenticate themselves when calling BCN's Help Desk prior to receiving service. The Help Desk authentication is not sufficient for the release of CPNI.

BCN does not share, sell, lease or otherwise provide CPNI to any of its affiliates, suppliers, vendors or any other third parties. Currently, BCN has a relatively small sales force that is primarily focused on selling its product through face to face meetings, and not primarily through any large-scale sales and marketing campaigns using CPNI. Sharing, selling, leasing or otherwise providing CPNI to any unrelated third parties is prohibited by the company as set forth in BCN's updated employee handbook of policies & procedures.

IV. Customer Consent.

In BCN's Customer Service Agreement, BCN includes language which allows for internal use of CPNI providing that the customer explicitly authorizes such use. In the event that the customer does not wish for their CPNI to be used by BCN for internal marketing (or "up-selling"), the customer may "opt out" which prohibits BCN from using their CPNI information for internal marketing. All customers who "opt out" have their accounts clearly marked to prevent any confusion.

V. Employee Training and Disciplinary Actions.

All personnel employed by BCN are required to participate in CPNI training. The goal of this training is to explain to employees what information is considered CPNI as well as what steps are necessary to protect and keep confidential any information defined as CPNI. Employees are required to sign an acknowledgment of receiving CPNI training which is added to their permanent employment file.

Severe disciplinary action will be taken against any employee who does not follow BCN's CPNI procedures. At present, this disciplinary action is immediate termination of the employee.